Paradigms and Prototypes

Security Policy Considerations for Justice Agency Executives
In the District of Columbia

Prepared by:
Information Technology Advisory Committee's
Privacy & Security Working Group

Karen Wallace, Chairperson
Earl Gillespie, ITLO
May 2000

Privacy and Security Working Group

Membership

Karen Wallace
Chairperson
Metropolitan Police Department

Dan Cisin
Assistant U.S. Attorney
U.S. Attorney's Office

Fred Doyle
Supervisory Computer Specialist
U.S. Attorney's Office

Raeford Grice
VB Programmer
Pretrial Services Agency

Leon Jackson
Chief Information Officer
Metropolitan Police Department

Tom Lord
Chief, Information Security
Policy & Information Resource Management
Federal Bureau of Prisons

Randall Moore
Youth Services Administration
Bureau of Court & Community Services

Jim Schenkenberg
Office of the Corrections Trustee

Blaise Supler
Deputy Trial Chief
Public Defender Services

Earl Gillespie
Information Technology Liaison Officer
Criminal Justice Coordinating Council

Anthony Arnold
Program Manager
Justice Grants Administration

Trip Hofer
Special Assistant
Criminal Justice Coordinating Council

Paradigms and Prototypes

Security Policy Considerations for Justice Agencies in the District of Columbia

Introduction

The *Interagency Agreement on Information Technology*, April 1999, is the platform from which the agency executives constituting the Criminal Justice Coordinating Counsel (CJCC) launched the development of integrated justice systems in the District of Columbia. This agreement, executed by the agency head of each of eleven justice agencies and the Chief Technology Officer, identified the basic information system concerns of the justice community, their resolve to establish an integrated system and to base that system upon certain principles.

Several of the principles recognized privacy and security issues. Those expressions included:

- The agreed objective is to share information which can be shared
- Significant amounts of information generated or processed by government agencies is restricted by reason of privacy protections, security restrictions and various privileges
- Each agency agrees to exercise due diligence in maintaining the integrity of both agency data and information system practices

The CJCC's Information Technology Advisory Committee (ITAC) carried those values forward to its *Mission and Goals*, where these objectives were established:

- Implementation of effective data and system security
- Respect for the confidentiality of information and individual privacy

The ITAC's commitment was put into practice with the establishment of the Privacy and Security Working Group (P&SWG). The role of the P&SWG was documented as:

> The role of the Security and Privacy Working Group (P&SWG) is to assemble the Security and Privacy documentation (including local and federal laws, regulations and rules) and formulate a plan of action for incorporation of security and privacy into the Justice Information System environment…. the Justice System would be incomplete and vulnerable without implementation of security and privacy

> standards. The security and privacy requirements of the justice community are complex and are not documented by a single set of standards nor set by a single source or authority. Further, standards recognized for years are changing in the recognition of fantastic advances in communications and access technology, broad new demands of public policy, and clarification of the information privacy rights of individual citizens.

This paper is intended to offer the justice community of the District of Columbia a brief examination of information related challenges, stimulate dialogue between and among personnel from different agencies with dissimilar assignments and varying levels of responsibility. This would offer an opportunity to achieve consensus and trigger plans of action to incorporate security and privacy requirements into the D.C. Justice Information System (JUSTIS) as well as the systems environment of participating agencies. This paper will suggest a variety of prototype policies that recognize issues raised by the "fantastic advances in communications and technology."

The information presented in this paper was drawn from a variety of sources. The Working Group discovered a surprising number of planning requirements and standards, most unknown to the majority of the agency representatives. An examination of resources offered a number of existing, often conflicting policy prototypes. Rather than engage in a futile attempt to somehow establish "Standards" or "Requirements" across functional, governmental and constitutional lines, the Working Group elected to suggest "Models" for ITAC and CJCC review and consideration. Some models lend themselves to implementation by individual agencies. Other models suggest action by the entire justice community.

Generally, each chapter will offer a model. These models are often an amalgamation of several prototypes and often reflect enthusiastic debate within the Working Group. The model represents the consensus of the Working Group. The model will be introduced with a discussion of the paradigm, circumstance or condition that necessitated it. In addition, where applicable, other prototypes that were discovered or other references, even templates, will be included in each chapter.

This paper should be considered perpetually incomplete. Chapters will be added as the CJCC and the ITAC express concerns about information system management and operation, or as they place requirements upon JUSTIS. The P&SWG will continue to monitor both changes to the criminal justice information system environment and documentation of additional requirements and standards. The P&SWG will be receptive to your suggestions to examine and identify privacy and security issues. Please forward suggestions to Ms. Wallace, Chair of the P&SWG, or Earl Gillespie, ITLO.

Appendix

Criminal Justice Information Systems, Article 27, Section 742, Maryland Code
CJIS Security Policy - NCIC
Criminal Justice Information Systems - CFR Title 28, Chapter 1, Part 20
District of Columbia Code – 1-1004, .5, 1-1521, 27 , 1-1522, 4-132, 135
District of Columbia Regulations – DCMR 1004.1, .4, .5
Freedom of Information Act
Interagency Agreement on Information Technology
Justice Department Vs Court Reporters Committee
Privacy Act of 1974
System Security Plan (SSP) Template (on disk)

Paradigms and Prototypes

Security Policy Considerations for Justice Agencies in the District of Columbia

The Information Technology Security Officer

Criminal Justice Information System (CJIS) policy is one of the responsibilities assigned by the U.S. Justice Department to the National Crime Information Center (NCIC) of the Federal Bureau of Investigation. The revised CJIS Security Policy dated March 1999, addresses agency adaptability and management of technological advances, specifically use of the Internet as a law enforcement tool. The CJIS Advisory Board recommended that the CJIS Division authorize a security management structure to specifically address technical security controls, security policy revision, oversight, training, and security incident notification. They also recommended that all criminal justice agencies establish an information security structure that provides an Information Security Officer at each Control Terminal Agency, Federal Service Coordinating Agency, and internationally, with the Interpol National Central Bureau. The result was the national implementation and maintenance of the Information Security Officer Program. The CJIS Security Policy Staff was also established to implement CJIS Security Policy and develop an Information Security Officer Training Program.

Several District of Columbia justice agencies have recognized the need for an agency Information Security Officer (ISO). Their policies mandated that the agency formally delegate responsibility for all information security matters. Often these policies state that the involved individuals may vary both cross or reside within existing organizational lines as long as there is a clear separation of responsibilities providing effective checks, balances, and accountability. However, each policy clearly states the importance of a single person being designated as having primary responsibility for coordination of agency information security and that another individual be designated as a backup.

The P&SWG ascribes the Information Technology Security Officer (ITSO) with responsibility for promulgating policies which establish security procedures and to audit to ensure compliance with those policies. The ITSO participates in the creation and review of policies and procedures, recommends security strategies (design, plan, procure), and keeps information systems current via continuous upgrades in technologies. The ITSO must ensure that his/her agency has established policies and procedures to prevent, detect, contain, and recover from information security breaches from both internal and external sources and

disasters, natural and otherwise. In order to be effective, the ITSO must also continue to pursue the most current levels of certification.

The Information Technology Security Officer should also have a coordination function. That person should be responsible for policy guidance, policy enforcement, and assistance in audits and systems design, publishing security related materials, and developing awareness programs. This staff function should report to the agency head or his/her designee who has responsibility across the entire organization. Some organizations have successfully placed this function in areas of audit, legal, or security. The IT security function should have one or more people working in this specialty, at least part-time. The responsibility for security rests with line management and should be stated clearly in the agency security policy.

Information is secure only when its integrity can be maintained, its availability ensured, its confidentiality preserved, and its access controlled. An ITSO is necessary in any organization where information systems contain sensitive data in need of protection against unauthorized intrusion inside and outside of the agency and where access is predicated upon a need to know basis.

City-wide ITSO Organizational Opportunities

While implementation of an ITSO program by an agency will certainly strengthen that organization, individual agency ITSO's do not increase the probability that the entire justice community will benefit from greater security. Strong individual security initiatives are just that, individual initiatives, not a community-wide security program. An example of a strong agency initiative, even if implemented in every justice agency, providing no additional community-wide protection or even endangering security, is the Logon.

The Logon is an identification code assigned an individual by the security custodian for an agency's records. For example, if Sam, an employee of MPD were to access WALES, he would need a Logon ID. The ITSO or Security Officer at MPD would assign a Logon, perhaps "Z99128" and a one-time password. Sam would then go to a workstation with access to WALES and would call up a screen to sign on to WALES. On it he would enter his Logon, Z99128, and his password. The system would verify that the Logon is valid and the password for that Logon is correct. This is an acceptable security measure.

But what if Sam required access with the PRISM system at CSOSA, and access to the system maintained by the DC Department of Corrections, and access to JUSTIS? Sam could be required to remember four different Logons, each with its different password. Sam will probably write the Logons down somewhere to aid his memory. This will also aid whoever would like to gain unauthorized access to the systems.

Part of the solution could be common Logon practices and/or standards for the entire justice community. For example, all agencies, as in the example above, could agree to use the same Logon policies and practices. None-the-less, even if that agreement were to happen, Sam's difficulty is not reduced. He is still required to obtain four different Logons: with agreement between agencies, he would obtain them using an identical procedure with each agency. (Sam is still writing each down to help his memory.) The difficulty is better addressed if there was only one Logon for Sam to remember.

A city-wide ITSO organization is best for each individual justice agency, and the community as a whole – certainly better for Sam. The ITSO organization provides the forum to identify, discuss and solve common security problems. The ITSO could address the problem of multiple Logons. The organization could agree on a common procedure for granting access between agencies and agree to issue one Logon for all system access by that user.

The D.C. ITSO Committee would identify problems, facilitate solutions and coordinate security related efforts city-wide. The members would provide a support mechanism for each other with technical and legal references and

referrals, unique skill sets, and knowledge of practical solutions. The DC ITSO Committee would serve the justice community by providing standards for security policies and procedures across agency boundaries, simplifying communication and reducing redundant or duplicative inter-agency practices. This committee would serve the citizens by giving security and privacy issues more priority. This committee would replace the Privacy and Security Working Group to become a more effective support group for ITAC.

Model Policy for the Information Technology Security Officer

POLICY:

1. CHIEF EXECUTIVE OFFICER. Each Agency Chief Executive Officer should appoint an Information Technology Security Officer (ITSO) to manage, ensure policy compliance, coordinate the overall District of Columbia Information Technology Security Program, and meet Program objectives. In addition, the appointing authority should notify the District's Privacy and Security Working Group (P&SWG) of the name of the designated ITSO.

Due to the broad scope of the responsibilities, knowledge requirements and dedicated time necessary to adequately fulfill the obligations of this position, it is recommended that an existing full-time position be utilized or an additional one created.

Additionally, each CEO should establish an Information Technology Security Committee for the Agency, to be chaired by an executive level employee. Members of the Committee would include at a minimum, the ITSO, Assistant ITSO's and system administrators.

2. INFORMATION TECHNOLOGY SECURITY PROGRAM OBJECTIVES.

The expected results of this program managed by the ITSO are that:

a. The acceptable security of information, computers and peripherals, workstations, terminals, telecommunications and data communications systems will be maintained.
b. Computer software installed on any Agency computer system will be legally purchased and licensed and used in compliance with the licensing agreement of the software vendor.
c. Staff who use or supervise the use of Agency computer systems will be informed about their responsibilities with regard to information and computer security and trained to meet those responsibilities.
d. All staff who handle sensitive information by any means, access computers or telecommunications systems in the performance of their duties, or supervise the use of such systems shall follow the procedures and meet the requirements of District of Columbia policy, Agency procedures and other applicable directives.

3. INFORMATION TECHNOLOGY SECURITY OFFICER RESPONSIBILITIES.

The Information Technology Security Officer (ITSO) will:

a. Manage and direct the Agency Information Technology Security Program. Report the program status to the CEO and the Privacy and Security Working Group.

(1) Establish and direct the local information security program, which encompasses the computer and telecommunications security programs. Ensure the implementation of security measures is commensurate with the sensitivity of information maintained at the site. Develop, and submit for the CEO's approval, written procedures for safeguarding sensitive information and systems. These procedures may take the form of a District of Columbia Policy Supplement, addendum to existing system security plans, or memoranda.

(2) Ensure that "Rules of Behavior" are developed and implemented for the Agency to provide employees with parameters for their activities and conduct concerning Agency systems use.

(3) Assist employees with information security matters, including safeguarding and marking sensitive information.

(4) Report security violations and virus infections to the CEO and the Privacy and Security Working Group (P&SWG). Minor violations (determined by the CEO) do not require a report to P&SWG. However, a description and disposition of the incident shall be documented and maintained locally. Using the proper format or other means prescribed by P&SWG and providing all required information concerning the incident, the following violations at a minimum should be reported to the CEO and P&SWG:

- Unauthorized access to District of Columbia or Agency computers or networks.
- Exceeding authorized access.
- Unauthorized software.
- Unlicensed software use.
- Introduction of malicious code.
- Unauthorized telecommunications and theft of services.
- Misuse or sharing of access IDs and passwords.
- Failure to properly protect or label storage media.
- Improper equipment and media disposal.
- Improper maintenance.

- Improper physical control of equipment, systems or information.
- Theft or destruction of computer resources.
- Improper use of system administrator privileges.
- Possession of prohibited subject matter.
- Utilizing the Internet for any illicit purpose.
- Unreasonable personal use of Agency systems.
- Using systems access for personal or non-Agency business.

It is the discovering ITSO's or Assistant's responsibility to notify other locations and ITSO's' Agencies that may become virus recipients or who may have originated the virus. The ITSO shall forward a copy of these notifications to P&SWG, unless included in the required report.

b. Recommend the designation of Assistant Information Technology Security Officers (AITSO's), as needed, to adequately implement and maintain the Information Technology Security Program. All LAN administrators should be appointed as AITSO's.

(1) Maintain a list of Assistant Information Technology Security Officers (ITSO's).
(2) Direct and determine the duties of the AITSO.
(3) Provide guidance to AITSO's concerning Information Technology Security and computer system media or hard copy documents containing sensitive information.

c. Systems Security Documentation.

(1) Coordinate and monitor performance of Agency computer risk analyses, system security plans, contingency plans, and compliance reviews.
(2) Provide guidance to system administrators in the development of system security plans and contingency plans, as required by Federal regulations. Contingency Plans are necessary to protect computer resources and ensure that essential functions continue if computer support is interrupted.
(3) Ensure security is adequately addressed, in accordance with District of Columbia policy, for areas with computer systems, automated or computerized telecommunications equipment such as PBXs, telephone switches, communications servers, modems, teletype terminals, and dial-up terminals or workstations.
(4) Make certain, as appropriate, system documentation is readily available to security officers, system managers, system administrators and users.
(5) Ensure that system and facility contingency plans/disaster recovery plans/continuity of operations plans are developed,

approved, initially tested within 90 days and then retested annually thereafter.

d. Systems Access Control.
   (1) Coordinate with the appropriate personnel official(s) and system administrator(s) and approve access to computer systems.
   (2) Ensure that the requesting individual has the permission of his or her immediate supervisor to request system access. This will establish the official need for access.
   (3) Ascertain that the minimum personnel security requirements have been satisfied prior to approving access.
   (4) Upon issue of IDs and passwords, advise users of their responsibilities concerning systems security and control of system access and associated passwords.
   (5) Affirm that the systems accounts of departing personnel are suspended. The disposition of the account and its contents will be determined by the immediate supervisor or higher.

e. Systems Backups.
   (1) Provide guidance to systems managers and administrators of the importance of systems backups.
   (2) Assist in identifying critical systems and information requiring regular backups.
   (3) Counsel system administrators on the frequency, storage, security and marking of system backups.
   (4) Ensure that system administrators develop and test procedures to restore data from backups as a contingency response to possible loss of original data.
   (5) Advise users on backup procedures for workstation hard drives when the data is not stored on network servers or mainframes.

f. Malicious Codes and Intrusion Detection.
   (1) Assure systems are protected from malicious programs and intrusions where feasible.
   (2) Review system needs for anti-virus and intrusion detection software. Currently, use of software for these purposes should be assessed for adequate safeguards.
   (3) Assist in determining frequency and appropriate use of security software products.
   (4) Ensure that all software patches and updates are regularly applied or installed.

g. Security Training and Awareness.
   (1) Comply with Federal and District of Columbia policy

requirements, tailoring subject matter to the Agency's needs and environment.

(2) Assess the resources and methods available to appropriately train Agency employees.

(3) In the best interests of the Agency and to the overall advantage of the security program, develop lesson plans, obtain computer based training or other training aids and provide or ensure that security training and awareness is provided to employees.

h. Systems Certification and Accreditation.

(1) Assume the responsibilities as the Certification Official for the Agency.

(2) Monitor, critique and assist with Certification and Accreditation activities.

(3) Advise Designated Accreditation Authorities (DAA) on their roles and guide them in the accreditation process.

I. Physical Security.

(1) Ensure that network servers and other critical system equipment are provided with safeguards sufficient to preclude physical access to systems and reduce the effect of current threats and vulnerabilities.

(2) As deemed appropriate, the ITSO will designate areas as computer rooms, specifying the criteria for the security of the systems to be protected.

(3) Monitor the placement of computer system screen displays for appropriate placement in order to guard against unauthorized viewing of or access to information or systems.

j. Media Security.

(1) Establish procedures that will ensure that electronic media is appropriately stored, handled, degaussed or destroyed prior to removal from secure areas within the Agency's control.

(2) Validate the adequacy of measures concerning media security and the clearing of data from electronic media.

(3) Approve methods and equipment used to secure sensitive media or clear media of critical or sensitive information.

(4) Ensure that approved shredders are available for the destruction of hard copy media and diskettes.

k. Program Review.

Conduct audits of Agency systems, facilities and procedures on an

annual basis to ensure compliance with District of Columbia and Agency policies and procedures.

4. Assistant Information Security Officer (AITSO)

(a) Perform the duties of the ITSO (as stated above) for a specific division, department, facility, office, location, computer system, or systems. At a minimum, the following individuals will be designated as AITSO's: all LAN administrators, PBX administrators, computer specialists, system administrators and communications technicians/specialists.
(b) Serve as Acting ITSO, if so designated or assigned.
(c) Report to the ITSO and the appropriate management official any changes or incidents involving computer systems that may affect the status of Information Technology Security.

Employees and E-Mail

The proliferation of e-mail in the workplace and the law governing employer's rights to monitor those communications is a case where technological developments in the workplace have outpaced applicable law and agency policies. E-mail has become the core of many employers' communications systems. At the same time, e-mail poses special problems for employers. The first of such problems involves the employee's expectation of privacy. This aspect of e-mail is difficult to discuss because it is surrounded by a mass of misinformation. "Electronic conversations," e-mail messages, including "erased" messages, provide crucial evidence in criminal and civil law actions. Examples include messages sent by an alleged sexual harasser, or perhaps restricted or sensitive communications sent between executives involving proposed disciplinary actions involving subordinates. Second, e-mail can be used by employees to divulge valuable trade secrets, intellectual property, or to infringe copyrights. Third, e-mail can distract employees who prefer to spend work time "chatting" with colleagues or friends.

Although federal legislation has been proposed to regulate employer monitoring of e-mail communications, employers currently have little direct guidance. The only federal statute that specifically addresses interception of e-mail communications is the Electronic Communications Privacy Act of 1986, which amended an earlier statue. The '86 statute expanded preexisting prohibitions on the unauthorized interception of wire and oral communications, to encompass electronic communications. The 1986 statue contains three exceptions that are particularly important to employers.

- First, and perhaps most important, the prohibition against intercepting communication does not apply where one of the parties to the communications consents to the interception. Consent may be implied where an employer puts its employees on notice that their electronic communication will be monitored.

- Second, the statute permits employers to intercept communication in the "ordinary course of business." In applying this exception, courts have looked at such factors as to whether the employer provided notice to the employees who were subject of the monitoring, whether the level of

monitoring was justified by the employer's legitimate business interests, and whether the communication was of a "business" nature.

- Third, the statue does not prohibit the interception of messages by the e-mail service provider, where the interception is necessary to provide the e-mail service or to protect the property rights of the provider. This exception is understood to mean that messages sent on completely "internal" company electronic mail systems are either not covered by the statue, or else have fewer protections than messages sent on more public systems.

The Fourth Amendment prohibits unreasonable search and seizure by the federal government and the Fourteenth Amendment, by state and local governments. In general, the Fourth Amendment requires "legitimate business needs" to justify a search. A search must then be limited to that necessary to advance the business justification. Normal business practices give employers fairly wide latitude to search employee work areas and personal effects. This is particularly true when the employer has previously disseminated rules that explicitly permit the search. Where this has been done, employees usually have been found not to have a reasonable expectation of privacy. By the same token, employer searches are more likely to be permitted where a company policy explicitly bans the conduct being investigated and thereby providing a legitimate reason for the search.

Some states have statues similar to the federal Electronic Communication Privacy Act. However, in practice, employees rely on a body of "common law" when attempting to challenge employer monitoring. This body of law typically prohibits the unreasonable intrusion upon the seclusion of another. In general, the question of whether an employer's "intrusion" concerns a sufficiently private matter to be objectionable depends upon whether the employee has a reasonable expectation of privacy. In a California case, the employer intercepted numerous e-mail messages, some of which were sexually explicit, sent between employees. Some employees sued claiming invasion of privacy. The appellate court rejected the employee's claims, relying on the fact that the employees had signed waivers stating "it is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business."

The internet article from which this paper was developed suggested that irrespective of where employers do business, federal, state, or private, all employers will improve their chances of surviving challenges to e-mail monitoring if the monitoring is tailored to be consistent with the business needs of the employer. In addition, that employees' privacy concerns are reduced by the dissemination of a policy that explains the extent to which the employer will monitor employees.

Regardless of the degree to which an agency will allow employees access and personal use of e-mail (or the Internet), to reduce the opportunity for misuse and subsequent liability for the agency, the following principles should guide the administrator:

- E-mail and/or Internet access are an agency owned resource provided for business purposes.
- The employee has no expectation of privacy in use of these agency owned resources.
- Certain uses and actions by the employee are explicitly prohibited.
- The agency will monitor these resources for misuse.
- The agency will take disciplinary action upon discovery of misuse by an employee.
- The employee will acknowledge the e-mail and/or Internet policy, in writing, prior to access and use of the resources.

CRIMINAL JUSTICE COORDINATING COUNCIL
Privacy and Security Work Group

E-Mail Access

Sample policy

The [criminal justice agency name], hereinafter referred to as the Agency is committed to providing an environment that encourages the use of computers and electronic information as essential tools to support criminal justice business. It is the responsibility of each employee to ensure that this technology is used for criminal justice purposes, proper business purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information. This policy covers all users of computer systems associated with the Agency.

E-Mail Procedures

- All E-mail correspondence (created, sent or received) is the property of the agency.
- Employee E-mail communications are not considered private regardless of designation either by sender or recipient.
- Messages sent to recipients outside of agency if sent over the Internet and not encrypted, are not secure.
- The agency reserves the right to monitor its e-mail system – including an employee's mailbox at its discretion in the ordinary course of business. In certain situations, the agency may be compelled to access and disclose messages sent over its e-mail system.
- Passwords and "message delete" functions do not restrict or eliminate the agency's ability or right to access electronic communications.
- Employee's shall not share an E-mail password, provide E-mail access to an unauthorized user, or access another user's E-mail mailbox without authorization.
- Employees shall not post, display or make easily available any access information, including, but not limited to, passwords.
- Offensive, demeaning or disruptive messages are prohibited. This includes but is not limited to, messages that are inconsistent with agency policies, specifically anti-discrimination policies concerning "Equal Employment Opportunity," "Sexual Harassment and Other Unlawful Harassment" (race, religion, politics, sexual preference, etc.)
- All broadcasts sent to the public, news organizations and others identified by the Public Information Officer require prior approval.
- All executive or administrative broadcasts require prior approval by appropriate member(s) of the agency.

ACKNOWLEDGEMENT OF E-MAIL ACCESS POLICY

As an employee of the _____(Criminal Justice Agency), I understand that the confidentiality and protection of Agency information is of utmost importance. I have read and understand the Agency Policy on acceptance and use of E-mail access.

If I received a password for access to E-mail, the Internet or any other system of electronically-stored computer information, I will use it only for authorized purposes. I agree not to use a code, access a file or retrieve any stored communication other than where explicitly authorized unless there has been prior clearance by an authorized representative of the Agency. I will notify Information Systems immediately if I believe that another person may have unauthorized access to my password.

I understand that all information stored in, transmitted or received through the Agency systems of printed or computer information is the property or the Agency, and is to be used only for job-related purposes. I further understand that authorized representatives of
the Agency may monitor the use of the Agency's systems of printed or computer information from time to time to ensure that such use is consistent with the Agency policies and interests. Further, I am aware that use of an Agency provided password or code does not in any way restrict the Agency's right or ability to access electronic communications.

_____
(Name)

_____
(Signature)

_____
(Date)

AND THERE ARE ALTERNATIVE VIEWS:

The P&SWG offers these policies as good sound business practices. We recognize their stringent nature, and are acutely aware that there are other less restrictive policies currently in practice by several participating agencies. However, as a first step, we suggest that the Agency heads review these policies and make only modifications that best suite their agency.

The difficulties with the more stringent policy model presented on the preceding pages are: 1) the policy is very difficult to monitor and enforce, and 2) if the agency fails to both monitor for misuse and enforce penalties, the agency is liable for not having done so. As a consequence, many agencies are allowing personal use of e-mail and Internet resources, with prohibitions such as those addressing harassment. Although this reduces the comprehensiveness of the monitoring required, it is not eliminated, and the liability for lack of monitoring and enforcement remains as great.

We understand that current agency business practices may or may not change to a great extent with access to e-mail and the Internet, but our policy objective is to reduce agency liability and meet federal mandates while offering quality technology tools in the business environment.

The following memorandums describe a less stringent approach to employee use of these new tools.

MEMORANDUM

SUBJECT: Personal Use of the Internet

We have received a number of inquiries about personal use of the Departmental Internet. As you may be aware the Department allows personal use of most office equipment where there is negligible cost to the Government and no interference with official business. Any personal use of Department property is subject to the overriding expectation that employees will give the government an honest day's work. This is covered in Management Regulation, nnn.nnn.nn. Personal use of the Internet is governed by the same rule.

In general, basic access to the Internet does not result in increased cost to the Department, and employees accordingly may use the Internet for matters that are not official business. For example, use of Internet e-mail is permitted because it does not result in additional cost. However, an employee making personal use of Internet e-mail should make it clear, when appropriate, that his or her e-mail is not being used for official duties.

On the other hand, employees are not authorized to make personal use of any of the Internet sites that result in an additional charge to the Government. These are generally identified as such when the user attempts to access them. It is the employee's responsibility to be aware whether an additional cost is involved.

Also, the Internet contains materials, such as sexually explicit material, that are not appropriate for the workplace. The Department expects employees to conduct themselves professionally in the workplace and to refrain from using Departmental resources for activities that are offensive to co-workers or the public.

Employees should also be aware that they have no expectation of privacy while using any Government-provided access to the Internet. The Department views electronic mail messages to be Government records, and it may have access to those messages whenever it has a legitimate Governmental purpose for doing so. Please also remember that all Internet communications identify the user to all sites accessed. Specifically, the sender is identified by his other complete Internet address, including the "xxxxxx.gov~ domain.

Finally, under NNN regulations, a supervisor may limit or revoke personal Internet use for any business reason.

If you have any questions about specific use of the Internet, please contact your supervisor.

MEMORANDUM

SUBJECT: Update on Personal Use of the Internet

The Department's Internet e-mail traffic has shown an increasing volume of traffic that does not appear to be related to the mission of the Department and which can slow the delivery of messages that are mission related. Employees are reminded that personal use of the Internet is allowed only to the extent that it does not interfere with official business. You should refrain from sending personal files that could slow the delivery of the Department's official Internet e-mail.

This type of traffic, which includes attachments such as automated greeting cards, image files, video clips, video games, and other executables, is particularly noticeable around the holiday. The problem can become particularly acute when large files are sent to more than one person at the same time. Even smaller files can slow official traffic when broadcast simultaneously to multiple destinations.

In addition, I would like to remind all employees of the danger of malicious software, which can be transmitted under the guise of a holiday greeting. Loading and executing any foreign software on your workstation, whether received in electronic mail, downloaded from the Internet, or given to you on a diskette, can result in damage to personal computers or in the compromise of sensitive Departmental information.

Finally, as I discussed in my previous memorandum on "Personal Use of the Internet," please make sure any personal files you send through the Departmental Internet connection are appropriate to the Department's workplace.

If you need further information on personal use of the Internet, please get in touch with your supervisor.

Employees and the Internet

Internet security takes many forms. Security includes hardware, the location of the Internet's physical components, anti-virus software, firewalls, and data encryption, even preparation for what to do in the event of a natural disaster. When the subject of Internet security arises, most IT managers and professionals focus on sophisticated technology rather than good solid IT management controls. IT management controls provide a great deal of protection, as they are the foundation for productive use of major sophisticated technological controls.

Internet security is protecting information assets from "accidental or intentional-but unauthorized-disclosure," modification, or destruction, and temporary unavailability. The publicity received by "hackers "and computer "viruses" has propelled the issue of protection of information on computers to public attention. Although this attention has been focused on the malicious external threat, the greater threat lies with "mistakes." Errors of omission and commissions by employees whose honesty is not in question, and who have been authorized access to the information, as part of their job is where the many difficulties lie. The major threat, established by a government study, is from employees when making honest mistakes. These errors are not only costly, but also are the training ground for the dishonest and disgruntled. Whereas the stranger or hacker, frequently commanding considerable attention, is the lowest threat. Controls for errors usually control both the employee and the stranger, although threats can vary significantly depending on the type of threat, the environment, and the nature of the application and data.

Most companies' computer users generally fall into one of three camps; those that are Internet "wizards"; those that are somewhat knowledgeable, but haven't had much experience with it; and those that have heard of it, know that great stuff is out there, but have no notion as to how to proceed. Most users are generally aware that there are security risks related to Internet use, but do not necessarily understand what the security issues are. They often do not know how to recognize a security problem or how to include Internet security procedures (rules of behavior) into their daily computer lifestyles. They may not know the consequences for inappropriate or unauthorized actions. Making computer systems users aware of their security responsibility and teaching them correct practices helps users change their behavior. Users cannot follow policies

they do not know or understand. Training also supports individual accountability, which is one of the most important ways to improve computer security. With out knowing the necessary security measures and how to use them, users cannot be truly accountable for their actions. Training is also needed for network administrators who need special skills to understand and implement the technology needed to secure Internet connections.

In a survey of 500 companies in the United States and Europe, it was found that on average, employees spend 1.2 hours per day on e-mail. It is estimated that more than 30 percent of employees spend more than 1.2 hours on the Internet and nearly 12 percent spend 2 hours per day on the Internet. With increased access and use of the Internet, "cyber-lollygagging" is what is now described as the workplace pastime. Employees with Internet access are spending considerable work time to explore the Internet. A study of workers revealed that they wasted between 20 and 60 percent of their time on the Internet. A survey by Nielsen Media Research revealed that on-line editions of Penthouse were called up thousands of times a month at major corporations like IBM, Apple Computer and AT&T.

The CIA's Foreign Bureau of Information Services implemented a policy in June of 1998 authorizing "electronic audits" of employee computers in order to crack down on non-business related Internet use. Those audits included reviewing employees' e-mail messages and collecting information on their Web site visits. A federal appeals court upheld a CIA policy allowing agency officials to monitor employees' Internet use. The policy had helped convict a federal employee of downloading child pornography on government time.

The increased use of e-mail and the Internet brings with it a number of risks and hazards for employers. Employers must be aware of the potential privacy rights of their employees, their rights or interest in monitoring employee use of e-mail and the Internet, potential liability for monitoring employee's-mail use, potential liability for employee conduct on an e-mail system, the potential for unauthorized disclosure of confidential information by employees or other third parties, the right of unions to access company employees via e-mail and in other issues relating to litigation. By all accounts, one of the best ways to manage the many risks and hazards presented by e-mail and the Internet is to maintain a formal policy that addresses these problems and establishes clear ground rules for the use of e-mail and the Internet.

CRIMINAL JUSTICE COORDINATING COUNCIL
Privacy and Security Work Group

Internet Access

Sample policy

The [criminal justice agency name], hereinafter referred to as the Agency is committed to providing an environment that encourages the use of computers and electronic information as essential tools to support criminal justice business. It is the responsibility of each employee to ensure that this technology is used for criminal justice purposes, proper business purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information. This policy covers all users of computer systems associated with the Agency.

Internet Procedures

- The Agency's (system name) network, including its connection to the Internet, is to be used for business-related purposes only and not for personal use. Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting, posting, or downloading pornographic material; engaging in computer-"hacking" and other related activities; attempting to disable or compromise the security of information contained on the Agency's computers or otherwise using Agency computers for personal use.
- Internet messages are to be treated as non-sensitive or private. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way, unless the messages are encrypted.
- Before posting information on the Internet, the information must reflect the standards and policies of the agency. Under no circumstances shall information of a restricted or private, sensitive or otherwise proprietary nature be placed on the Internet.
- Subscriptions to news groups and mailing lists are permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.
- Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.
- Employees may not establish Internet or other external network connections that could allow unauthorized persons to gain access to Agency systems and information unless the prior approval of the Agency has been granted. These connections include the establishment of hosts

with public modem dial-ins, World Wide Web home pages and File Transfer Protocol (FTP).

- All files downloaded from the Internet must be scanned for possible computer viruses.
- Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with Agency policies concerning “Equal Employment Opportunity,” “Sexual Harassment and other Unlawful Harassment” (race, religion, politics, sexual preference).

Any employee who violates this policy shall be subject to discipline, up to and including discharge.

ACKNOWLEDGEMENT OF INTERNET ACCESS POLICY

As an employee of the _____(Criminal Justice Agency), I understand that the confidentiality and protection of Agency information is of utmost importance. I have read and understand the Agency Policy on acceptance and use of E-mail and Internet access.

If I received a password for access to E-mail, the Internet or any other system of electronically-stored computer information, I will use it only for authorized purposes. I agree not to use a code, access a file or retrieve any stored communication other than where explicitly authorized unless there has been prior clearance by an authorized representative of the Agency. I will notify Information Systems immediately if I believe that another person may have unauthorized access to my password.

I understand that all information stored in, transmitted or received through the Agency systems of printed or computer information is the property or the Agency, and is to be used only for job-related purposes. I further understand that authorized representatives of
the Agency may monitor the use of the Agency's systems of printed or computer information from time to time to ensure that such use is consistent with the Agency policies and interests. Further, I am aware that use of an Agency provided password or code does not in any way restrict the Agency's right or ability to access electronic communications.

_____
(Name)

_____
(Signature)

_____
(Date)

Paradigms and Prototypes

Security Policy Considerations for Justice Agencies in the District of Columbia

Pre-Employment Checks

While gathering references and information for other chapters of this paper from the Internet, the subject of pre-employment background checks often was included in search engine results. In the justice information system environment background checks are universally considered a tenet of system access security requirements. The P&SWG assumption was that such checks, more specifically criminal history background checks, were routinely completed for all justice employment opportunities. That assumption was naive.

While no formal poll was completed, general discussions indicated that criminal history checks were not completed prior to granting access to many agency information systems. In addition, pre-employment background checks, including criminal history, were not as routine as one might expect. Agency heads may wish to reexamine this apparent void in personnel policies for a variety of reasons. Reasons include:

- good management practices
- business liability issues
- system access restrictions related to criminal history record information (CHRI).

The background check, as a good management practice, is suggested by one company in statistics offered on their web page: employee theft causes 30% of business failures; the workplace is the scene of over 30 million crimes and thefts each year; one third of applicants submit an employment application containing false information. Another source quoted 1994 applicant figures that included: 18% had criminal records, 20% had suspended licenses, 14% had DUI's, 29% had falsified educational claims, 7% had never worked for a referenced employer, and 14% of employers, when checked, indicated they would never rehire that employee.

In a litigious society, the potential for liability cannot be easily dismissed. While personnel with the appropriate legal training best discuss liability issues and implications, the uninitiated can follow the terms and definitions. The term "negligent hiring" can be defined as "the failure of the employer to exercise reasonable care in selecting an applicant in light of the risk created by the position to be filled." Quite often cases involving negligent hiring relate to the premise that negative facts in a person's background should have precluded him/her from a given position.

Restrictions on personnel allowed access to CHRI are found in the Code of Federal Regulations (CFR) relating to Criminal Justice Information Systems, as well as the *CJIS Security Policy* of the Criminal Justice Information System (CJIS) of the National Crime Information Center (NCIC) division of the FBI. The CFR clearly states a criminal justice agency has the right to reject for employment all personnel who have direct access to CHRI, based upon good cause. Although the term "good cause" may be arguable, the System Security Policy of CJIS/NCIC states, "Thorough background screening by the employing agency is required. State and national lll record checks by fingerprint identification must be conducted. Good management practices dictate record checks should be completed prior to employment. If a record of any kind is found, access will not be granted."

The P&SWG would encourage all justice agencies to perform background checks, not limited to, but including criminal history record and warrant checks on every employee prior to employment. However, because the mission of this Working Group relates to justice information systems, the Model Policy addresses only access to JUSTIS.

Model Policy for Pre-Employment Record Checks

MODEL POLICY:

Fingerprint supported criminal history record checks and warrant checks must be completed for all personnel allowed direct access to JUSTIS, prior to employment. Where personnel are currently employed, fingerprint supported criminal history record checks and warrant checks must be completed prior to direct access to JUSTIS being granted.

The criminal history record check is to be conducted on city, federal and NCIC files.

If the record check appears to indicate a fugitive want or a warrant, the agency head or his/her designee will review the matter. Access will not be granted to JUSTIS until the matter is resolved.

If a felony record is found, access to JUSTIS will not be granted.

If a misdemeanor is found, the matter will be referred to the agency head or his/her designee for review. Access will not be granted until the matter is resolved.

Further restrictions on access to the files of each agency are the responsibility of the agency identified as custodian of that data.

Further restriction on access to national files including, but not limited to, NCIC and NLETS are the responsibility of the Metropolitan Police Department.

Paradigms and Prototypes

Security Policy Considerations for Justice Agencies in the District of Columbia

System Security Planning

System security planning activities are neither unique nor recently applied to justice agencies. While all government information systems have evolved through security plans and practices over the years, the justice community had the earliest set of security requirements placed upon their "people based" systems. The justice system security regulations, and security planning requirements, were initiated with the development of computerized criminal history (CCH) efforts under the Law Enforcement Assistance Act (LEAA). This led to the Privacy Act of 1974 and the Code of Federal Regulations, Title 28, Chapter 1, part 20, *"Criminal Justice Information Systems,"* March 1976.

These laws and regulations were followed by numerous other sets of requirements and standards. A recent lecture by a guest expert identified:

- Privacy Act of 1974 and 1978
- Federal Regulation 11714,1976
- Federal Managers Financial Integrity Act of 1986
- Computer Security Act of 1987
- Paperwork Reduction Act of 1995
- Paperwork Elimination Act of 1998
- Presidential Decision Directive #63
- OMB Circular A-123
- OMB Circular A-130
- NIST and NSA / NCSC Standards

Other associated government requirements as well as unique city laws, regulations and standards join this long list. These are all further supplemented by a myriad of agency standards, requirements and practices.

How to follow all of these laws, regulations, requirements, and standards? How to simply discover that they exist and learn how they affect your agency? How to prepare for audits? How to avoid penalties?

These questions were common ground for confusion, differing opinions, and conflicting practices, but elicited few facts. The P&SWG invited a technical assistance expert in system security planning, under contract to GSA, to come to our meeting and share the facts about planning with us. Our guest expert offered that a variety of agencies are prepared to offer technical guidance. The presentation identified as many as twenty agencies and divisions at the Federal

level alone that are prepared to offer this guidance. Each can provide voluminous sets of data, booklets, bulletins and documentation. In addition, at least five Federal agencies or divisions are prepared to offer technical assistance. However, each offers this assistance on a "fee for service" basis.

The speaker suggested that an agency primed to tackle the planning requirement must start preparing for the planning requirement as early as when the system is being conceptualized. The security planning is to be considered integral to the initial steps of system planning. The speaker suggested the system security planning process has a minimum of five steps:

1. Map privacy & security requirements
2. Develop privacy & security policies
3. Conduct and document a risk assessment
4. Select and document counter measures
5. Prepare and commit to a security plan

The District of Columbia's Justice Information System (JUSTIS) faces the same system security planning challenge as each of the participating agencies. Perhaps the method and approach that JUSTIS will use may be a practical model for those agencies.

JUSTIS faces the standard test of just preparing a plan that meets all those requirements and standards. That challenge is joined by two other circumstances. The first is that several other states which have developed integrated systems using a variation of the Internet technology / browser / middleware theme have experienced a great deal of difficulty demonstrating to users the rationale for the high level of security required when accessing CHRI. The second is the proof of concept (POC) or pilot system JUSTIS will initially implement will be without other than rudimentary system security. This status cannot be permitted into the second phase; therefore JUSTIS must conduct a thorough system security requirements analysis and system security functional analysis.

These circumstances create an opportunity for JUSTIS to identify all the security requirements and standards, and clearly explain the elevated CHRI access security standards to the potential users, thus avoiding much of the opportunity for conflict seen in other states. This analysis will also identify each of the requirements and standards that will be the focus of an auditable system security plan. That planning process will highlight the functional requirements of the system inasmuch as those standards must be translated into technology, procedures and policies. The result will be informed users, a detailed System Security Plan (SSP) that will pass muster from both Federal and NCIC audits, and implementation of a secure system honoring the principles of the *Interagency Agreement of Information Technology.*

The JUSTIS approach to the SSP and the functional analysis will be based upon the technical assistance offered by GSA. That agency has a system security

expert vendor under contract and available to provide technical assistance to the justice agencies in the District of Columbia, on a fee for service basis. This vendor may be procured through special venues which avoid a protracted SOW / RFP procurement process.

Should a participating agency not have an acceptable system security plan and elect to prepare the plan with in-house resources, a valuable planning enabler is available at no cost. Mitretek has prepared a very detailed template for the SSP. A sample of that template can be found in the appendix of this paper. A disk with the complete template is included, on disk, with this booklet. If an agency desires to use the SSP approach that JUSTIS will follow, the ITAC representative should contact the ITLO for the name and phone number of the associate with the expert vendor utilized by GSA for technical assistance.

Model Policy

Pursuant to the Computer Security Act of 1987 and the Privacy Act of 1974, the ___Agency Name_____ will prepare a System Security Plan (SSP) consistent with the standards, guidelines, policies and regulations appropriate to this system activity. The SSP will identify and include each agency system that gathers, stores, manipulates, disseminates or otherwise manages sensitive data.

The responsibility for preparing the SSP will be assigned the agency's Information Technology Security Officer (ITSO). Agency personnel and vendor technical assistance approved by the agency head will assist the ITSO. The ITSO will prepare a project plan and schedule for review and approval to proceed. The SSP will be completed and presented for review within ninety (90) days of approval to proceed.

The SSP shall be transmitted to the National Institute for Standards, Technology (NIST), and the National Security Agency (NSA) for advice and comment. The plan must be reviewed by an independent agency such as the Office of Management and Budget (OMB).

The SSP shall be reviewed annually and revised as appropriate. Certification of the review and documentation of any revisions will be submitted to the agency head.

Model Table of Contents for the System Security Plan

Table of Contents

SECTION **PAGE**

3.0 OPERATIONAL CONTROLS
3.1 Personnel Security
3.1.1 Access Authorization
3.1.2 Limited Access
3.1.3 Individual Responsibility
3.1.4 Individual Identification
3.1.5 Visitors in Controlled Areas
3.1.6 Termination/Debriefing
3.2 Physical and Environmental Protection
3.2.1 Location
3.2.2 Access Control
3.2.3 Data Interception
3.2.4 Document Storage Containers
3.2.5 Combinations Locks
3.2.6 End-of-Day Security Checks
3.2.7 Individual Responsibilities
3.2.8 Personal Items in Secure Areas
3.2.9 Package Inspection
3.2.10 Equipment/Material
3.2.11 Custodial and Maintenance Procedures
3.2.12 Emergency Medical Notification
3.2.13 Fire Safety Factors
3.2.14 Failure of Supporting Utilities
3.2.15 Structural Collapse
3.2.16 Plumbing Leaks
3.2.17 Use of Other Building Facilities
3.3 Production, Input/Output (I/O) Controls
3.3.1 User Support
3.3.2 Procedures to Prevent Unauthorized Access
3.3.3 Procedures to Ensure Authorized Access
3.3.4 Audit Trails for Receipt of Sensitive Inputs/Outputs
3.3.5 Procedures for Restricting Access to Output Products
3.3.6 Procedures and Controls Used for Transporting Output
3.3.7 Internal/External Labeling for Sensitivity
3.3.8 Labeling
3.3.9 Document Control
3.3.10 Media Storage
3.3.11 Procedures for Sanitizing Electronic Media for Reuse
3.3.12 Procedures for Controlled Storage, Handling, or Destruction of Media that Cannot Be Effectively Sanitized for Reuse
3.3.13 Procedures for Shredding or Other Destructive Measures
3.4 Contingency Planning
3.4.1 Business Plan
3.4.2 Identify Resources
3.4.3 Develop Scenarios

3.4.4 Develop Strategies

3.4.5 Implement Strategies
3.4.6 Test and Review Plan
3.4.7 Information Backup Procedures
3.4.8 Computer Security Incident Handling
3.5 Application Software Maintenance Controls
3.6 Data Integrity/Validation Controls
3.6.1 Virus Detection and Elimination Software
3.6.2 Reconciliation Routines
3.6.3 Password Crackers/Checkers
3.6.4 Integrity Verification
3.6.5 Intrusion Detection Tools
3.6.6 System Performance Monitoring
3.6.7 Penetration Testing
3.6.8 Message Authentication
3.7 Documentation
3.8 Security Awareness and Training
3.8.1 Identify Program Scope, Goals, and Objectives
3.8.2 Identify Training Staff
3.8.3 Identify Target Audiences
3.8.4 Motivate Management and Employees
3.8.5 Administer the Program
3.8.6 Maintain the Program
3.8.7 Evaluate the Program

4.0 TECHNICAL CONTROLS
4.1 Identification and Authentication
4.1.1 Identification
4.1.2 Authentication
4.1.3 Audits
4.1.4 Trusted Paths
4.2 Logical Access Controls
4.2.1 Authorization or Restriction of User Activities
4.2.2 Granting Access Rights
4.2.3 Establishing ACL or Register
4.2.4 Restricting Access to Operating System
4.2.5 Detection of Unauthorized Transactions
4.2.6 Automatic Blanking of Screen
4.2.7 Passwords
4.2.8 Encryption to Prevent Access
4.2.9 Connectivity with Internet or Other WANs
4.2.10 Constrained User Interfaces
4.2.11 Gateways or Firewalls

4.2.12 Port Protection Devices

4.2.13 Internal Security Labels
4.2.14 Host-based Authentication
4.2.15 Warning Banners
4.3 Public Access Controls

Appendix A: System Security Personnel

Appendix B: Rules of Behavior

Appendix C: Applicable Systems Policies and Procedures Incorporated by Reference in the SSP

Appendix D: Sample Glossary and List of Acronyms

Review & Challenge

Q. The offender has the right to come in and demand to see his/her criminal history record (CHRI)? They actually can demand to see it? They can challenge what they see in the record - even if my agency did not place the information in that record? They can make an agency change the data because they claim it is incorrect?

A. Yes, yes, yes and yes!

Access and dissemination are the focal points for much of the misunderstandings and confusion found in any discussion of CHRI. This model policy section will concentrate on access. Further, the access policy question under discussion is limited to access by the individual of record, commonly identified as the "offender."

Discussions of access to data about a particular individual can be centered on one or more pieces of Federal legislation and regulation. Prominent in these discussions are the ***Freedom of Information Act*** (FOIA), the ***Privacy Act of 1974*** (Privacy Act) and Title 28, Chapter I, Part 20, ***Criminal Justice Information Systems*** (CJIS CFR), of the Code of Federal Regulations. While there are hundreds of interpretations and guides to the FOIA and Privacy Act, the model policy this chapter addresses is limited to criminal history record information (CHRI). For a discussion of FOIA and the Privacy Act, please see the section on "Public Access."

It is important for each agency to determine if data collected, stored, manipulated and disseminated by the agency is CHRI. If the data is classified as CHRI, numerous conditions regarding all processing activities, including review and challenge, come into play. The CJIS CFR defines CHRI as:

> (b) Criminal history record information means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising there from, sentencing, correctional supervision, and release.

It is significant that the CHRI definition has just two parameters: identification and notations. As a consequence, if a record identifies an individual and contains

data regarding a criminal justice process, it is prudent to assume the data is CHRI. It is also essential to note that the definition does not include limitations regarding storage or delivery media. Nowhere in the definition is CHRI restricted to automated (computerized) information; the CHRI definition is not nullified because the data is in a manual system, or perhaps simply a file folder, a 3x5 card.

If CHRI exists, the CJIS CFR requires processes by which the individual of record may review and challenge that CHRI.

> g) Access and review. Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that-
> (1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;
> (2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;
> (3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;
> (4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;
> (5) The correction agency shall notify all criminal justice agencies of the corrected information; and
> (6) The individual's right to access and review shall not extend to data contained in intelligence, investigatory or other related files and shall not be construed to include any other data not defined in § 20.3(b).

The policy maker should note that the individual of record may not only require the agency to correct his/her CHRI, but also take two additional steps:

1. require the agency to provide the names of all non-criminal justice agencies (entities) to whom his/her record had been disseminated, and
2. notify all criminal justice agencies (to which the data had been disseminated) of the correction.

Neither this section, nor the CJIS CFR, addresses the requirements and processes associated with the FOIA or the Privacy Act and/or their relationships to CHRI. Each of those laws, and how they address CHRI, are unique and have no direct bearing on the agency's responsibility to the individual of record under the CJIS CFR.

The next pages provide a model policy and a model procedure. The “policy” was drawn directly from a state law designed to reflect the CJIS CFR and the “procedure” was drawn from the state regulation enabled by that state law. While neither may be directly applicable to a particular criminal justice agency in the District, they provide sufficient detail to allow an agency executive or record custodian to begin to recognize how extensive the requirements, complexities and practical implications of the CJIS CFR are.

A significant note to the agency executive is that these models are only “half” the required policies and procedures. These models address the review and challenge process from the perspective of an agency, with only passing reference to the Central Repository. The Central Repository is truly “central” to this process. The policy, and more importantly, the myriad of procedures allowing and reacting to an individual’s right to review and challenge, CHRI correction, notification, and audit are much more complex for the Repository. This paper does not attempt to address them except to indicate where the Repository procedures must be congruent with agency expectations.

Model Policy: Right of inspection and Challenge

Review and Challenge

Inspection

A person may inspect criminal history record information maintained by a criminal justice agency concerning him/her.

Before an individual may review his record he will verify his identity by fingerprint comparison.

A person's attorney may inspect such information if he satisfactorily establishes his identity and presents a written authorization from his client.

Nothing in this section requires a criminal justice agency to make a copy of any information or allows a person to remove any document for the purpose of making a copy of it. A person having the right of inspection may make notes of the information.

Challenging information

Notice of challenge -- A person who has inspected criminal history record information relating to him may challenge the completeness, contents, accuracy, or dissemination of such information by giving written notice of his challenge to the agency at which he inspected the information, if other than the Central Repository. The notice shall set forth the portion of the information challenged, the reason for the challenge, certified documentation or other evidence supporting the challenge, if available, and the change requested in order to correct or complete the information or the dissemination of the information. The notice shall contain a sworn statement, under penalty of perjury, that the information in or supporting the challenge is accurate and that the challenge is made in good faith.

Audit of information; notice of repository's determination. Upon receipt of the notice, the agency shall conduct an audit of that part of the person's criminal history record information necessary to determine the accuracy of the challenge. The agency shall notify the person of the results of its audit and its determination within 90 days after receipt of the notice of challenge. This notice shall be in writing, and, if the challenge or any part of it is rejected, the notice shall inform the person of his rights of appeal.

Correction of records. If the challenge or any part of it is determined to be valid, the agency shall make the appropriate correction on its records, and shall notify any criminal justice agency that has custody of the incomplete or inaccurate information, or portion of it, of the correction, and that agency shall take appropriate steps to correct its records. The notified agency shall certify to the agency that the correction was made

Notice of correction when information is disseminated. A criminal justice agency required to correct any criminal history record information that had previously disseminated such

information shall give written notice to the agency or person to whom the information was disseminated of the correction. That agency or person shall promptly make the correction on its records, and certify to the disseminating agency that the correction was made.

Notice to agencies of denial of challenge. If the challenge, or any part of it, is denied, the agency shall give written notice of the denial to any agency with which a copy of the challenge was filed.

Inspection or challenge of information relevant to pending criminal proceeding. A person is not entitled to inspect or challenge any criminal history record information if the information or any part of it is relevant to a pending criminal proceeding. This subsection does not affect any right of inspection and discovery permitted under any statute, rule, or regulation not part of or adopted as part of this policy.

Rights of appeal.

Rules for administrative appeals -- The agency shall adopt appropriate rules and procedures for administrative appeals from decisions by criminal justice agencies denying the right of inspection of, or challenges made to, criminal history record information.

These rules shall include provisions for
(1) The forms, manner, and time for taking an appeal;
(2) The official or tribunal designated to hear the appeal;
(3) Hearing and determining the appeal; and
(4) Implementing the decision on appeal.

Right to take administrative appeal. A person aggrieved by a decision of a criminal justice agency concerning inspection or a challenge may take an administrative appeal in accordance with the rules and procedures adopted by the agency.

Right of an Individual to Inspect Her/His Criminal History Record

A. A person may inspect criminal history record information concerning him maintained by a criminal justice agency, unless the information or any part of it is relevant to a pending criminal proceeding. This latter restriction does not affect any right of inspection and discovery permitted by rule of court or by statute.

B. A fee of $nn, payable to the agency will be charged an individual for each request to review his record, unless he individual files a verified certificate of indigency.

C. If an individual wishes to file a request and subsequently review his criminal history record at the agency, he may do so 9 am through 3 pm, Monday through Friday, except on city or Federal holidays. An individual may review and challenge his record only at a municipal criminal justice agency in the District of Columbia or the Central Repository.

D. Until all criminal history data is filed at the Central Repository, an individual may file a request and subsequently review that part of his criminal history record maintained by a criminal justice agency at other than the Central Repository. This request and review is subject to the procedures of the criminal justice agency that maintains the record. Each criminal justice agency that maintains criminal history record information shall adopt procedures for individual review and challenge of that information. These procedures will be in compliance with applicable Federal and State law and regulations.

E. An offender held in custody at a law enforcement agency, detention center, or correctional institution as the result of a court action may file a request and subsequently review his criminal history record at the location of his confinement.

F. Before an individual may review his record he will verify his identity by fingerprint comparison by the Central Repository.

G. Any attorney may review his client's criminal history record if he satisfactorily establishes his identity and presents a written authorization from his client.

I. The Central Repository will verify the identity of the applicant.

J. Upon confirmation of the identity of the applicant by fingerprint comparison and other available identifiers, the Central Repository shall complete an identification verification form and return it and a copy of any record information within 30 days to the agency that submitted the request.

K. The Central Repository or other agency possessing the individual's criminal

history record may deny review of a record if, in its opinion, the individual cannot satisfactorily identify himself as the subject of that record, or if the individual is not entitled to review the record under the limitations set forth in the Review and Challenge Policy. The Central Repository or other agency that denies access shall return a written response to the individual within 30 days will indicate the reason for denial on form. The individual will be advised in writing of his right to appeal the denial of review.

L. The Central Repository will retain a copy of the verification form.

M. When an individual returns to review his criminal history record, he shall countersign the verification form. An individual inspecting his criminal history record may make notes of the information or may obtain a certified copy at his expense.

N. A person who challenges his criminal history record information may challenge the completeness, the contents, the accuracy, or the dissemination of this information.

Right of an Individual to Challenge A Denial to Inspect

A. If an individual is denied the right to inspect his criminal history record, pursuant to the procedures in the procedure above, he may challenge this denial in accordance with the procedures in this regulation. This regulation does not pertain to court procedures or court records where the courts have denied inspection.

B. A fee of $nn, payable to the agency will be charged an individual for each request to challenge his record, unless the individual files a verified certificate of indigency.

C. An individual shall file a challenge to a denial of his request to inspect his record by submitting Challenge Form and a complete set of fingerprints taken at the location of his original request by the original agency. An individual shall file a challenge within 10 days of the denial to inspect his record.

D. The Agency Head has the authority to designate a review officer.

E. The Agency Head shall set a review date within 30 days of the date the challenge is filed, and within the 30-day period the full set of fingerprints submitted by the person who challenged the record will be compared with the fingerprints on the arrest record.

F. The Agency Head will issue to the individual and to the Central Repository a written decision stating whether the individual filing the challenge is the individual in the record. The Central Repository will retain a copy of the decision and copies will be disseminated by the Central Repository to any other agency that is a party to the denial process.

G. If the Agency Head decides that the challenger is identical to the individual in the record, the challenger may, upon submission of the written decision of the Superintendent to the official who denied access to the record, view his record.

H. If the Agency Head decides that the challenger is not the individual in the record, the challenger may not be permitted to inspect the record.

I. The challenger, or the agency maintaining the record, may appeal the decision of the Agency Head and this appeal shall be taken in accordance with the Review & Challenge Policy.

Right of an Individual to Challenge Completeness, Contents, Accuracy, and Dissemination

A. An individual who has inspected his criminal history record information may challenge the completeness, content, accuracy, or dissemination of this information.

B. A fee of $nn, payable to the agency, shall be charged an individual for each challenge to the completeness, contents, accuracy, and dissemination of his criminal history record, unless the individual files a certified certificate of indigency.

C. The individual will submit the Challenge Form as notice of his challenge to the Central Repository and to the agency at which he inspected the information, if other than the Central Repository. Upon receipt of the Challenge Notice, the Central Repository will conduct an examination of that part of the person's criminal history record information that has been challenged as to completeness, contents, accuracy, and dissemination. As part of the examination, the Central Repository may require any criminal justice agency that was the source of challenged information to verify the information. The Central Repository will advise the person of the results of its examination and its determination within 90 days after receipt of the individual's notice of challenge. This notice shall be in writing if the challenge or any part of it is rejected, the notice will inform the person of his rights of appeal.

D. If the challenge is determined to be valid, the Central Repository will make the appropriate correction on its record and notify any criminal justice or other agency that has custody of the incomplete or inaccurate information, of this correction. The criminal justice agency shall correct its records and certify to the Central Repository that the correction was made.

E. A criminal justice agency or other agency required to correct any criminal history record information that had previously disseminated this incorrect information shall give written notice of the correction to any agency or individual to whom the information had been disseminated. The recipient agency or individual will promptly make the correction on its records, and certify to the disseminating agency that the correction was made.

F. If the individual's challenge to the completeness, contents, accuracy, or dissemination is denied by the Central Repository, he may appeal the decision in accordance with the procedures outlined below.

G. A fee of $nn, payable to the agency, will be charged an individual for each request to appeal a denial of his record, unless the individual files a verified certificate of indigency.

H. Within 30 days of a denial, an individual will file Challenge Appeal form to appeal a denial of a challenge with the criminal justice agency which contributed or created the record, if other than the Central Repository.

1. The Agency Head has the authority to designate a hearing officer.

J. The Agency Head shall set a hearing date within 30 days of the date the appeal was filed, and the hearing shall be held within 60 days of the date the appeal was filed.

K. Failure of an applicant to appear at the hearing shall be cause to deny the challenge.

L. At the challenge hearing, the applicant who filed the challenge and any agency party to the challenge may be represented by an attorney, may introduce additional evidence, and may interrogate persons responsible for recording or maintaining the criminal history record in question.

M. The Agency Head shall issue to the applicant and to the Central Repository a written order stating the decision of the hearing. A copy of the order shall be retained by the agency and disseminated by the Central Repository and to any other agency or person who is party to the hearing.

N. If the Agency Head concludes that the challenge to the completeness, contents, accuracy, or dissemination of the record is correct, the order will direct that the record be corrected. The Central Repository and the criminal justice agency that contributed or created the record shall correct its records and certify to the Agency Head that the correction was made.

O. A criminal justice agency required to correct any criminal history record information that had previously disseminated this information, shall give written notice to the agency or person to whom the information was disseminated, of the correction. That agency or person shall promptly make the correction on its records, and certify to the disseminating agency that the correction was made.

P. Any party to the matter may further appeal the decision of the Agency Head, and this appeal shall be taken in accordance with the City or Federal Administrative Procedure.

Public Access

Review and Challenge policy speaks to what CHRI must be provided an individual of record maintained by an agency. That policy does not engage in guidance concerning what information regarding an offender and/or an event can an agency share with the public. What inquiries about an offender and/or event can be answered? These questions are distinctly different from issues surrounding the requests by the individual of record, yet the answers share common circumstances – the definition of criminal history record information, CHRI.

First review the definitions found in Title 28, Chapter I, Part 20, declaring what is, and is not, CHRI. The definition of CHRI has two qualifiers, identification and data relating to a criminal justice process:

> "Criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising there from, sentencing, correctional supervision, and release.

Later in the regulation, additional criteria are offered; each disqualifying certain uses of data or certain records from being restricted by the CHRI definition, and which sets the stage for a discussion of dissemination.

> (b) The regulations in this subpart shall not apply to criminal history record information contained in:
> (1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;
> (2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis;
> (3) Court records of public judicial proceedings;
> (4) Published court or administrative opinions or public judicial, administrative or legislative proceedings;
> (5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of

> regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses;
> (6) Announcements of executive clemency.
> (c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

The regulation then addresses the subject of dissemination of non-conviction CHRI. Relevant portions of the regulation state:

> (b) Limitations on dissemination. Insure that dissemination of non-conviction data has been limited, whether directly or through any intermediary only to:
> (1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;
> (2) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, as construed by appropriate State or local officials or agencies;
> (3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement…...
> (4) Individuals and agencies for the express purpose of research…

The regulation concludes the dissemination discussion with "general policies":

> (c) General policies on use and dissemination. (1) Use of criminal history record information disseminated to non-criminal justice agencies shall be limited to the purpose for which it was given.
> (2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.
> (3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

The regulatory passages addressing dissemination of CHRI has a history of contentious questions from both the record custodians and those who wanted access. The circumstances when data is, and then is not CHRI required clarification. In the ***Commentary on Selected Sections of the Regulations on Criminal History Record Information,*** published in 1976, the following discussion was offered:

> Sec. 20.20 (b) and (c). Section 20.20 (b) and (c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know. Court records of public judicial proceedings are also exempt from the provisions of the regulations. Section 20.20(b)(2) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.
>
> Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1975" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal justice agency may respond to the inquiry. Conviction data as stated in Sec. 20.21(b) may be disseminated without limitation.

Unfortunately for the policy maker, the CHRI regulation is not the only government policy on public access and dissemination. Adding to the dissemination discussion is the complication that portions of both the ***Freedom of Information Act*** (FOIA) and the ***Privacy Act of 1974*** also appear to address CHRI.

The Privacy Act has only two general exceptions to the information that may be requested from a government agency by the public.

> The first applies to all records maintained by the Central Intelligence Agency. The second applies to selected records maintained by an agency or component whose principal function is any activity pertaining to criminal law enforcement. Records of criminal law enforcement agencies

> can be exempt under the Privacy Act if the records consist of (A) information compiled to identify individual criminal offenders and which consists only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) criminal investigatory records associated with an identifiable individual; or (C) reports identifiable to a particular individual compiled at any stage from arrest through release from supervision.

Therefore, the Privacy Act uses the same definition of CHRI as the Regulations, and clearly states that CHRI cannot be obtained through application of this law. To this CHRI exception, the Privacy Act adds investigatory records and all processing records that include identification data. As a consequence, the Privacy Act creates no circumstances requiring an agency policy or procedure granting access to CHRI.

The FOIA also has identified data that is excluded from consideration for dissemination. One exemption, Number 7, has six specific circumstances where access to data is restricted.

> Exemption 7.--Law Enforcement
>
> The seventh exemption allows agencies to withhold law enforcement records in order to protect the law enforcement process from interference. The exemption was amended slightly in 1986, but it still retains six specific sub-exemptions.
>
> Exemption (7)(A) allows the withholding of a law enforcement record that could reasonably be expected to interfere with enforcement proceedings. This exemption protects an active law enforcement investigation from interference through premature disclosure.
>
> Exemption (7)(B) allows the withholding of information that would deprive a person of a right to a fair trial or an impartial adjudication. This exemption is rarely used.
>
> Exemption (7)(C) recognizes that individuals have a privacy interest in information maintained in law enforcement files. If the disclosure of information could reasonably be expected to constitute an unwarranted invasion of personal privacy, the information is exempt from disclosure.
>
> Exemption (7)(D) protects the identity of confidential sources. Information that could reasonably be expected to reveal the identity of a confidential source is exempt. In addition, the exemption protects information furnished by a confidential source if the data was compiled by

> a criminal law enforcement authority during a criminal investigation or by an agency conducting a lawful national security intelligence investigation.
>
> Exemption (7)(E) protects from disclosure information that would reveal techniques and procedures for law enforcement investigations or prosecutions or that would disclose guidelines for law enforcement investigations or prosecutions if disclosure of the information could reasonably be expected to risk circumvention of the law.
>
> Exemption (7)(F) protects law enforcement information that could reasonably be expected to endanger the life or physical safety of any individual.

These exemptions relate more to law enforcement data and activities than directly to CHRI. In fact, neither the term "criminal history" nor the definition of "identification plus records or notations, etc." appear in the exemption language. Exemption (7) (C) is a near as the FOIA comes to a CHRI category or definition. The significance of this lack of direct linking with the other CHRI characteristics or dissemination restrictions establish the foundation for a challenge. That challenge was answered within a Supreme Court decision.

When access to "Rap Sheets" (CHRI) held by the FBI was requested under the FOIA by a CBS correspondent and the Reporters Committee for Freedom of the Press, the request was rejected. The decision was challenged. The U. S. District Court supported the Department of Justice position. The Court of Appeals reversed. The Supreme Court reversed the Court of Appeals. Justice Stevens delivered the opinion of the Court.

> The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that, in today's society, the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains the age of 80, when the FBI's rap-sheets are discarded…..
>
> What we have said should make clear that the public interest in the release of any rap-sheet…that may exist is not the type of interest protected by the FOIA…
>
> [T]he privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap-sheet is a private citizen, and when the information is in the Government's control as a compilation, rather than as a record of "what the Government is up to," the privacy interest protected by Exemption 7(C) is, in fact, at its apex, while the FOIA-based public interest in disclosure is at its nadir. . . . Such a disparity on the scales of justice holds for a class of cases without regard to individual circumstances. . . Accordingly, we hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be

> expected to invade that citizen's privacy, and that, when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted." The judgment of the Court of Appeals is reversed.

The decision makes it clear that Rap Sheet data, i.e. CHRI, is not available through FOIA inquires. All this discussion leads back to the questions that opened this review, " What information about an offender and/or event can an agency share with the pubic? What inquiries about an offender and/or event can be answered?" What data can be disseminated and what questions can be answered in response to FOIA and Privacy Act requests? An agency need look no further and the CHRI CFR.

MODEL POLICIES

Access to CHRI is a complex matter. Issues such as public announcements, press releases, response to questions by the press, and sharing of data to promote and support cooperative efforts between justice and non-justice agencies need careful examination. The agency executive responsible for such policies is encouraged to directly enlist legal assistance and to examine polices from other agencies in the District of Columbia as well as those similar agencies in other states.

The model policies below address issues not related to the press and are offered to encourage further examination and definition.

Issue 1 General dissemination policy

Policy: The following general principles apply to access to CHRI:

- the direct access to CHRI is limited to authorized criminal justice officials.
- No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.
- Use of criminal history record information disseminated to non-criminal justice agencies shall be limited to the purpose for which it was given.

Issue 2 Inquiries for CHRI by the individual of record

Policy: See Chapter on “Review and Challenge”

Issue 3 Inquiries for CHRI based upon the Freedom of Information Act (FOIA)

Policy: The FOIA prohibits a third party request for law enforcement records about a private citizen. FOIA inquiries for CHRI will not be honored.

Issue 4 Inquiries for CHRI based upon the Privacy Act of 1974

Policy: The Privacy Act grants an exception to third party inquiries for records meeting the definition of CHRI. Privacy Act inquiries for CHRI will not be honored.

Issue 5 Direct Access to CHRI

Policy: Direct access to CHRI is limited to authorized personnel of a criminal justice agency.

Direct access means having the authority to access the criminal history record database, whether by manual or automated methods.

Criminal justice agencies include the Courts and any government agency or any subunit that performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

The administration of criminal justice means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information. State and Federal Inspector General Offices are included.

Issue 6 Access to non-conviction data

Policy: Dissemination of non-conviction data is prohibited to other than:

- authorized criminal justice personnel or any intermediary for purposes of the administration of criminal justice and criminal justice agency employment;
- individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order;
- individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement;
- individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency.

Paradigms and Prototypes

Security Policy Considerations for Justice Agencies in the District of Columbia

Misuse of Justice Data / Systems

Systems developed for criminal justice agencies and the data collected and maintained on those systems are particularly sensitive. As a consequence, justice agencies must make significant investments in comprehensive measures to protect those resources. Unfortunately, no technical security measure effectively protects the data from misuse by employees. Each justice agency must construct misuse policies and penalties every bit as robust and effective as their technical security measures and should be used in conjunction with Office of Management and Budget Circular -130 on Rules of Behavior.

This chapter will attempt to discuss policies that define employee misuse, identify penalties and suggest legislation. One of the paradoxes of justice data is that while there are a multitude of sanctions that can be imposed against agencies for a large number of misuses, the sanctions against personal misuse, if any, penalize the agency rather than the individual. It is assumed the agency must have appropriate policies regarding misuse. Even more ironic, in many states it is arguable that misuse of data, much less justice data, is even illegal.

Each agency must develop information system security policies that address potential misuse. Each policy should utilize the term “unauthorized” use to differentiate between agency sanctioned employee activities and activities which are considered misuse. This will help avoid confusion in a circumstance where an employee is authorized to access data for agency purposes, but must be penalized when he/she uses that same access for activities the agency does not authorize.

In addition, to avoid liability, the agency must monitor for activities which agency policies declare unauthorized. Further, the agency must penalize personnel whose activities are discovered through that monitoring process. The agency faces liability if there are damages for which the agency took no action to avoid, or if the agency documented actions, but did not follow up on the agency responsibilities to penalize.

The chart ***Misuse of Data and/or Systems*** suggests agency policy might include, but not be limited to, seven areas of unauthorized activities. Each prohibited action is paired with an appropriate reaction by the agency for each circumstance. The issues are sorted from the most serious to the least serious:

Misuse of Data and/or Systems

Action	Reaction				
Form of Misuse	**Prosecution**	**Suspension**	**Permanent Loss of Access**	**Written Reprimand**	**Loss of Access Pending Training**
Misuse in Commission of a Crime	X	X	X		
Misuse that Damages Data or a System	X	X	X		
Misuse that Damages Another Person		X	X	X	
Misuse for Personal Advantage		X	X	X	
"Theft" of Data			X	X	X
Recreational Misuse				X	X
Inadvertent Misuse					X

- Misuse in Commission of a Crime

  This is the use of justice information to support a criminal activity. An obvious example would be the use of address data to support a breaking and entry, or an assault, or the use of criminal history to extort. Less obvious is the selling of justice information to insurance agents, private investigators and employment bureaus.

  The agency's reaction to this unauthorized use must include supporting prosecution activities and suspension of the employee pending the outcome of prosecution and trial. Regardless of trial verdicts, the agency must permanently take access from the employee for cause; breach of public trust.

- Misuse that Damages Data or a System

  This includes unauthorized activities by an individual that destroy, erase, modify or falsely enter data on any agency information system, or cause any physical damage to any central equipment, workstations, lines, communication or security devices.

The agency must pursue prosecution for damages to any system. It is arguable that in some states the employee can be prosecuted for damaging data. The agency must suspend the employee pending trial verdict, and must permanently take access from the employee for cause; breach of public trust.

- Misuse that Damages another Individual

  This policy prohibits the use, while not illegal, of any information from a justice system that causes harm to another person, and for which the agency may be held liable. An example would be disclosing the relationship between an individual and an offender with a criminal history. Disclosing that a husband has a criminal record might prevent a wife from obtaining a personal loan, or disclosing a citizen's non-conviction records might damage an employment opportunity for that individual.

  An employee making unauthorized use of justice information that damages an individual is to be immediately suspended. The employee is to permanently lose access to justice systems for cause; breach of public trust. A written reprimand is to be placed in the employee's permanent personnel record.

- Misuse for Personal Advantage

  The unauthorized use of justice data for personal advantage must be strictly prohibited. This one issue is often recognized by employee as "wrong", but at the same time, the employee sees the unauthorized use as justified and part of the privileges of the employment – much like taking home office supplies. An example would be the father who does a record check on his daughter's boyfriend, or the mother who does a check on the new next-door neighbor.

  While this unauthorized use arguably does not "damage" another individual, it remains an unauthorized access for other than criminal justice purposes and the employee obtains data which he or she would not have been able to obtain if not employed by the justice agency. The employee should be suspended and permanently lose access to the justice system for cause; breach of public trust. A written reprimand is to be placed in the employee's permanent personnel record.

- "Theft" of Justice Data

  This "theft" is not one defined in criminal code. If it were, then the first policy would be appropriate. This theft is unauthorized use of data for purposes other than for which it was collected. This unauthorized use frequently does no harm to another individual, and is not illegal, per se. However, it is a breach of public trust inasmuch as the data is used for purposes other than the citizen understood it was collected, or for which the agency was authorized to collect. An example would the employee who is drawing up a mailing list for his/her high school reunion, or the employee who looks up friends and acquaintances birth dates so he/she might send cards on time.

  This breach of public trust is compounded by the employee's use of agency resources for personal use. The employee should lose access for cause; breach of public trust. The loss of access may be for a period of time rather than permanent. If not a permanent loss, the reinstatement should be permitted only after completing refresher training on proper use if justice systems. A written reprimand is to be placed in the employee's permanent personnel record for personal use of agency resources.

- Recreational Misuse

  This unauthorized use more often relates to misuse of a system or workstation, perhaps affecting system capacity, response time or ability to contact the user. While the unauthorized use is very minor in impact, without penalty, this type of misuse can lead to substantial system utilization and could lead to more serious unauthorized use. This is not too different from an employee using an agency automobile for personal use or sending a subordinate on personal errands. An example of this type of unauthorized use is the employee who runs friends and neighbors names just to see if there are any hits, or the employee who forwards jokes and or gossip to other employees.

  Recreational misuse of justice resources, while minor, should not be permitted not go without penalty. The employee should have a written reprimand placed in his/her personnel file. Agency policy should determine if the reprimand is permanent or should remain for only a certain period of time. The employee should lose access until he or she has completed a refresher course on the proper use of justice systems.

- Inadvertent Misuse

  Inadvertent misuse is often characterized as "dumb" use. An untrained employee, an employee with general training in a circumstance where

specific training was necessary, or where policy was too general, typically commits the misuse. Because the agency has contributed to the potential misuse by not having properly prepared the employee, the agency must share the responsibility for the misuse. An example of this type of misuse is when an employee without authorized access to certain data or systems, is asked to "cover" for another employee because of an emergency. The temporary employee does not have a password to access the data/system so another employee's password is used. Another example is when an employee who, as part of his duties, is constantly leaving a room, but was never informed of a policy that requires an employee to log off any workstation when it is not in use. As a consequence, the workstation is open to unauthorized access every time the employee leaves.

These seven areas of discussion are suggested as the foundation for defining unauthorized use of systems and data for employees. These are not comprehensive, nor are the penalties necessarily those appropriate to an agency's traditional practices or such limitations as union agreements.

Legislative Foundations for Misuse Policies

The broader issue is whether certain unauthorized use of data or systems is illegal. The discussion of illegal use of data transcends justice data; it is more appropriately discussed within the realm of "Public Records." This follows the logic that although all records in government are public records, some are set aside, subject to special restrictions. Some laws make a distinction between record that are automated and those that are not.

Both model laws on the following pages address unauthorized access and use of data. In the first law, the data is that in a "public record." This law is rather short and straightforward, and applies only to government records, whether automated or not. After editing, and removing definitions, the intent, in (b) is:

> It is unlawful to make a false entry in a public record, or without authority alter, deface, destroy, remove, conceal or access a public record.

The second model law more carefully address computer oriented system and data. This law is lengthier, has a greater number of definitions, and is not restricted to governmental records. The intent of the law is clearly defined in section (c):

> "No person shall intentionally, willfully, and without authorization access, Attempt to access or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services."

PHYSICAL SECURITY for COMPUTER WORKSTATIONS

The security requirements identified here represent a basic prerequisite to providing a secure computer workstation operating environment and ensuring the privacy and security of the Criminal Justice Information System information.

A formal security training program must be in effect which regularly provides all employees training in security awareness, impact of current privacy legislation, emergency procedures, and backup and contingency operations. This training program must include scheduled orientation training for all new employees.

Physical security regarding computer workstations is indeed a very broad topic and has the potential to take us in many different directions. An example of which is the NCIC Physical Security Policy that addressed the computer site, visitors of computer centers and terminal workstations as well as specific requirements for authorized personnel. Other physical security policies are quite extensive and cover everything from passwords to disaster recovery. However, best practices for computer workstation security indicates that the best protection is through self-audits. Physical security policies should include the following relevant requirements:

* The conditions under which access authority is granted to criminal justice information assets must be available to all personnel with the responsibility of protecting those assets.

* Access to computer rooms/workstation environments and criminal justice information storage areas must be tightly controlled at all times.

* A list of all personnel with authorized access to the computer rooms/workstation environments and criminal justice information storage areas must be available to all personnel responsible for or working in those areas.

* All entrances (including windows to the computer rooms/workstations environments and criminal justice information storage areas must either be under 24 hour surveillance or fitted with effective anti-intrusion devices (such as bars, locks, alarms, etc.).

The following Security Self-Assessment guide is apart of the Physical Security/Computer Workstations policy and is provided for your consideration. The Guide is offered as a useful resource and enables criminal justice agencies to apply corrective actions where appropriate. Keep in mind that this Self-Assessment Guide is not a substitute for an independent on-site audit. On the other hand, full compliance with the items included in the self-audit will indicate that you have significantly reduced your risk exposure.

Model Self Assessment

Security Issues Related to Workstations with Access to CHRI

SECURITY MANAGEMENT

YES NO N/A 1. Has responsibility for the security of the workstation equipment and CHRI been designated in writing with a description of duties?

YES NO N/A 2. Is there a written overall workstation and CHRI security plan to use as the basis for correcting recognized security deficiencies and implementing new controls?

YES NO N/A 3. Are workstation and CHRI security concerns normally considered in all proposed and actual facility changes?

YES NO N/A. 4. Are all people who use the workstation or the CHRI data aware of their responsibilities for maintaining its security?.

YES NO N/A 5. Are all security related incidents directed toward either this workstation equipment or the CHRI records followed up with an appropriate investigation, report, and an indication of corrective actions taken?

YES NO N/A 6. Are the locations of workstation rooms and CHRI records processing and storage areas sown played, such that they are not prominently marked or publicized?

YES NO N/A 7. Is the authority to access the workstation room(s) and the CHRI processing and storage area(s) granted only after a management review of the requirement for access?

PERSONNEL PRACTICES

YES NO N/A 8. Are all employees who will have access to workstation equipment and CHRI subjected to a background check for honesty and integrity prior to being given such access?

YES NO N/A 9. Are employees who have access to workstation

Equipment and CHRI and are to be terminated or reassigned, restricted from access to workstations and CHRI following their notification of termination?

YES NO N/A 10. Are safe and code combinations changed immediately and workstation passwords cancelled, and keys collected, upon the termination or reassignment of an employee with those combinations, keys, or valid passwords?

YES NO N/A 11. Are non-employee personnel (such as visitors, vendors, custodians) required to be escorted at all times while they may have access to workstation equipment or CHRI?

YES NO N/A 12. Do employees routinely challenge the presence of people in the workstation room or the CHRI processing area who are not assigned to the workstation room or CHRI processing section?

ADMINISTRATIVE PROCEDURES

YES NO N/A 13. Are workstation instruction manuals treated as sensitive information and adequately secured at all times?

YES NO N/A 14. Are the CHRI processing functions separated from other functions of the organization?

YES NO N/A 15. Are the CHRI records controlled and maintained separately from the other records of the organization?

YES NO N/A 16. Are there written instructions available to those employees who deal with the security and storage of CHRI?

YES NO N/A 17. Are CHRI records secured when not in constant use, such as at night, on weekends, or when not needed?

YES NO N/A 18. Are workstation screens situated such that the CHRI displayed is normally not visible to persons without a need-to-know?

YES NO N/A 19. Are CHRI documents in use on desks, tables, etc. protected from disclosure to persons without a need-to-know (i.e., from a service window)?

YES NO N/A 20. Are CHRI documents which are no longer needed destroyed in a proper manner?

YES NO N/A 21. Are recipients of written copies of CHRI required to sign a receipt?

YES NO N/A 22. Are the number of carbon or reproduced copies of CHRI tightly controlled?

TRAINING

YES NO N/A 23. Do all new employees with access to the workstations or CHRI receive training on the organization's security and confidentiality policy, procedures, and practices?

YES NO N/A 24. Is there a formal security training program in operation which provides scheduled training to all employees on security awareness, emergency procedures, and back-up and contingency actions?

YES NO N/A 25. Are employees regularly trained (at least annually) in fire prevention and suppression techniques?

YES NO N/A 26. Are employees trained in emergency and power failure procedures?

PHYSICAL ACCESS

YES NO N/A 27. Are there written procedures detailing the conditions under which personnel are to be authorized access to the workstation equipment and CHRI?

YES NO N/A 28. Are employees familiar with the authorization approval procedures for new access authorization requests?

YES NO N/A 29. Are there specific security procedures and practices enforced which control access to workstation rooms and CHRI storage areas?

YES NO N/A 30. Are these controls in effect 24 hours a day, seven days a week?

YES NO N/A 31. Are all visitors (personnel not assigned full time) to the workstation rooms and CHRI processing and storage

areas required to sign in and out?

YES NO NIA 32. Is there a written authorization list, available to the CHRI processing supervisor, of personnel who have been granted access to the CHRI?

YES NO N/A 33. Is there a written authorization list, available to the workstation supervisor and operators, of personnel who have been granted access to the workstation equipment?

YES NO N/A 34. Are all entrances (including windows) to the workstation rooms and CHRI processing and storage area filled with effective anti-intrusion devices (bars, locks, alarms, shatterproof glass, guards, etc.)?

YES NO N/A 35. Are unguarded doors and windows kept locked at all times?

HAZARD PROTECTION

YES NO N/A 36. Are the areas adjacent to the workstation room kept free of combustible trash, cleaning materials, and flammable supplies?

YES NO N/A 37. Are the areas adjacent to the CHRI processing and storage areas kept free of combustible trash, cleaning materials, and flammable supplies?

YES NO N/A 38. Is the workstation room itself kept clear of excessive combustible materials and supplies?

YES NO N/A 39. Is the CHRI processing and storage area kept clear of excessive combustible materials and supplies?

YES NO N/A 40. Are fire prevention and fire fighting procedures posted for all employees?

YES NO N/A 41. Are portable fire extinguishers located strategically throughout the workstation room and CHRI processing and storage areas?

YES NO N/A 42. Are fire extinguishers regularly inspected?

YES NO N/A 43. Are portable fire extinguishers of a size light enough for all employees to use effectively?

YES NO N/A 44. Are smoke detectors installed in the workstation room and CHRI processing area?

YES NO N/A 45. Do smoke and fire alarms sound at a location which is manned 24 hours a day?

YES NO N/A 46. Is there a "no smoking or drinking" policy enforced at the workstation equipment?

YES NO N/A 47. Is the electric power supply sufficient to provide adequate backup power for the workstation room?

YES NO N/A 48. Are power distribution panels locked or otherwise secured to prevent unauthorized access, yet afford accessibility in an emergency?

TELECOMMUNICATIONS

YES NO N/A 49. Is access to valid workstation passwords controlled and protected so as to prevent unauthorized personnel from obtaining them?

YES NO N/A 50. Is the display or printing of the access password always suppressed so that it does not appear on the workstation screen or on a printout?

CONTINGENCY PLAN

YES NO N/A 51. Are backup CHRI documents (such as microfiche, original or copies of documents), retained and stored in a secured container or area separate from the working documents?

YES NO N/A 52. Have arrangements been made in writing to use an alternate workstation should the on-site workstation(s) be non-operational?

YES NO N/A 53. Is there a written contingency or disaster plan available in several copies to the key personnel which addresses workstation operation and CHRI processing.

YES NO N/A 54. Do key personnel have a copy of the plan at home?

YES NO N/A 55. Are all workstation operators and CHRI processing employees knowledgeable of their duties and responsibilities during emergency operating conditions?

YES NO N/A 56. Has an individual been designated in writing as the contingency or disaster planning officer, with specific assigned duties?

YES NO N/A 57. Have there been any tests of the disaster plan, if so, have the results been documented and used improve the plan?

YES NO N/A 58. Are emergency telephone numbers posted for employees to use?

YES NO N/A 59. Are key personnel backed up with trained alternates capable of performing the same job?

Legislative Opportunities and Considerations

This Paradigms and Prototype document was prepared by the ITAC's Privacy and Security Working Group with the overall objective to offer the justice community of the District of Columbia opportunities to:

- conduct a brief examination of information related challenges,
- stimulate dialogue between and among personnel with differing assignments and varying levels of responsibility within participating justice agencies,
- achieve clarity through consensus on definitions and classifications,
- trigger a plan of action to address the challenges.

The "models" offered in each section are central to this objective. Each agency is invited to compare and contrast their policies with these models. Agencies without prior policy development should consider the models as incentive to develop policies specifically addressing agency requirements. Prior to any attempt to either re-write existing policy or create new policies, justice agency executives should review both District of Columbia law and regulations and the Criminal Justice Information System (CJIS) regulations.

As important as individual agency policies are, it is perhaps more important to have consistent definitions, classifications and designations in analogous policies across local and federal agencies. Nationally, the foundation for that consistency has been the CJIS Regulation. This chapter examines that regulation and the District's justice community's opportunity to build upon that same foundation.

On ten occasions since 1974, a national analysis of state privacy and security legislation has been conducted. The analyses are based upon surveys examining how comprehensively each state has addressed the issues that were the causal underpinning of the Federal regulation on Criminal History Information Systems (CJIS CFR). The CJIS CFR was categorized into 28 survey aspects. The results of the survey were last presented in ***The Compendium of State Privacy and Security Legislation: 1997 Overview***, prepared by SEARCH Group, and published by the Bureau of Justice Statistics. The Compendium has been edited for this paper to present a comparison between the legislative environment for CJIS in the District of Columbia and that environment in the other states. The CJIS CFR can be found in the Appendix.

Three charts from the Compendium follow this page. The first chart identifies the 28 subject matter categories that are representative of the primary topics of the CJIS regulation. The second chart, "Comparison of Changes," identifies the number of states that have addressed each of the 28 CJIS subject matter categories through legislation. You will note that the number of states with such legislation has increased dramatically since the initial survey in 1974. The third chart, representing only the District of Columbia, indicates a paucity of supporting law and regulation in those same 28 categories. A copy of the laws and regulations referenced in this chart are found in the Appendix.

The information in these charts demonstrate a need for the District of Columbia criminal justice community to examine opportunities to establish, and clarify where appropriate, the city's laws and regulations for each of the 28 subject matter categories through a mutually agreed upon set of standard definitions, classifications and responsibilities.

A strong foundation from which the justice community can build the future is through District of Columbia legislation for Criminal Justice Information Systems. To do so, an assembly of specialists is required. They must have expertise in:

- the unique functional relationships between the District's justice agencies,
- practical solutions to justice processing dilemmas,
- the vocabulary of the District's justice process,
- records and information system management requirements,
- insight into the citizen's needs and requirements,
- national criminal justice system responsibilities,
- standards for criminal justice information systems established by national regulations and laws.

The District is fortunate in that all areas of expertise, save one, are currently represented by the participating agencies of the Criminal Justice Coordinating Council. That one area of expertise not covered, Federal law and regulation affecting criminal justice information systems, is easily obtainable. What is most critical to this initiative, and has been absent to date, is a system-wide recognition of this critical need and the will to address the challenge.

Model Legislation

Title 28, Chapter I, Part 20, Criminal Justice Information Systems (CJIS) in included in the appendix to this document. It is the seminal document for all state and local codes, laws and regulations on the subject. As witnessed by the survey results in the Compendium, virtually every state has incorporated appropriate sections of this Title from the Code of Federal Regulations (CFR) in their state law, regulations and procedures.

While the selection of available state CJIS laws is large and varied, a single state law is offered for consideration as a model. The section of this particular state law was based upon four criteria: the law closely parallels the CJIS CFR, the law establishes a governance structure very similar to the governance structure developed by the District, expertise and additional information regarding legislative intent is easily accessible, and the ITLO has had experience with this particular law.

APPENDIX

Criminal Justice Information Systems, Article 27, Section 742, Maryland Code
CJIS Security Policy - NCIC
Criminal Justice Information Systems - CFR Title 28, Chapter 1, Part 20
District of Columbia Code – 1-1004, .5, 1-1521, 27, 1-1522, 4-132, 135
District of Columbia Regulations – DCMR 1004.1, .4, .5
Freedom of Information Act
Interagency Agreement on Information Technology
Justice Department Vs Court Reporters Committee
Privacy Act of 1974
System Security Plan (SSP) Template (on disk)

Criminal Justice Information Systems, Article 27, Section 742, Maryland Code

CJIS Security Policy – NCIC

Criminal Justice Information Systems - CFR Title 28, Chapter 1, Part 20

District of Columbia Code – 1-1004, .5, 1-1521, 27, 1-1522, 4-132, 135

District of Columbia Regulations – DCMR 1004.1, .4, .5

Freedom of Information Act

Interagency Agreement on Information Technology

Justice Department Vs Court Reporters Committee

Privacy Act of 1974

System Security Plan (SSP) Template (on disk)